

FIG. 1

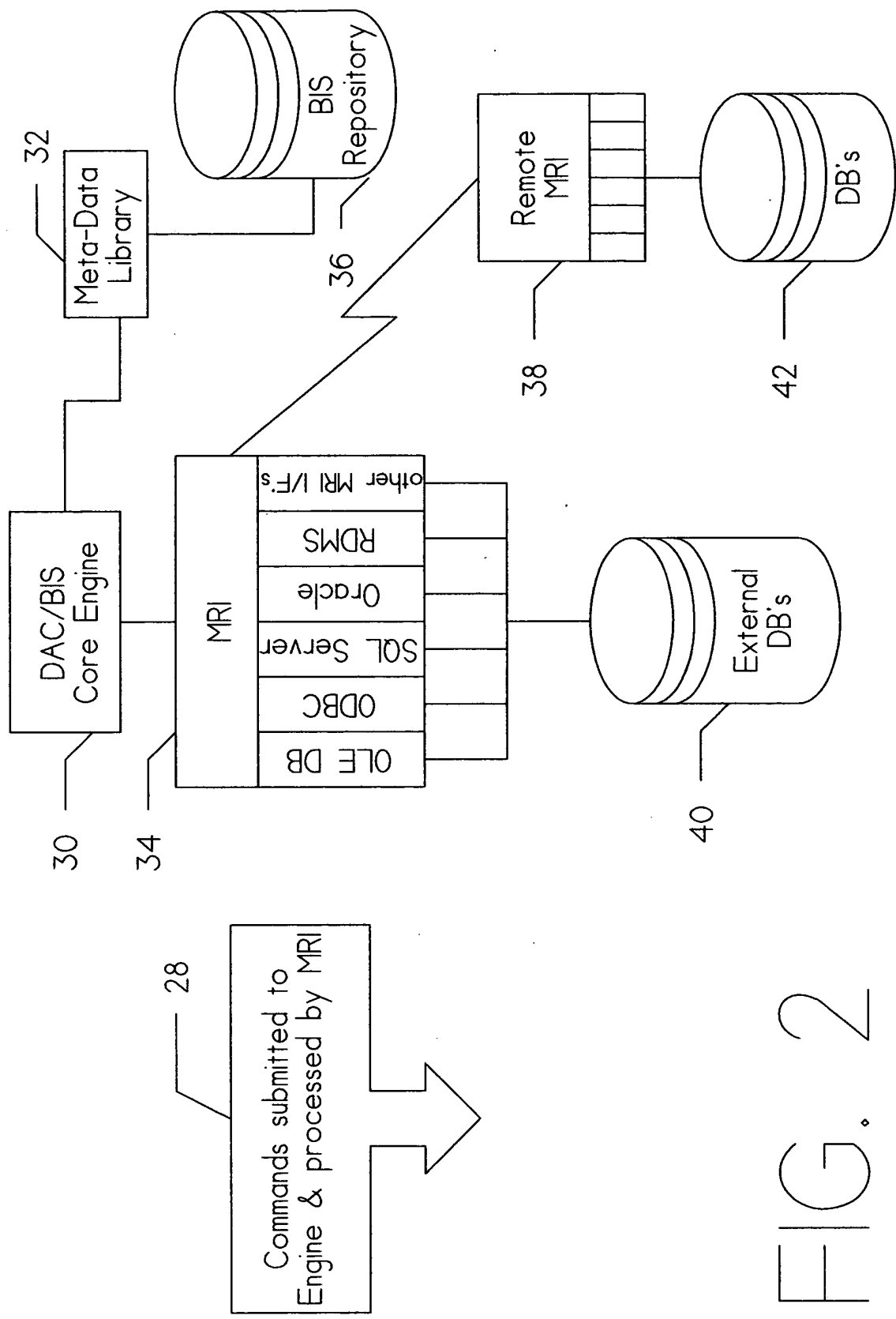
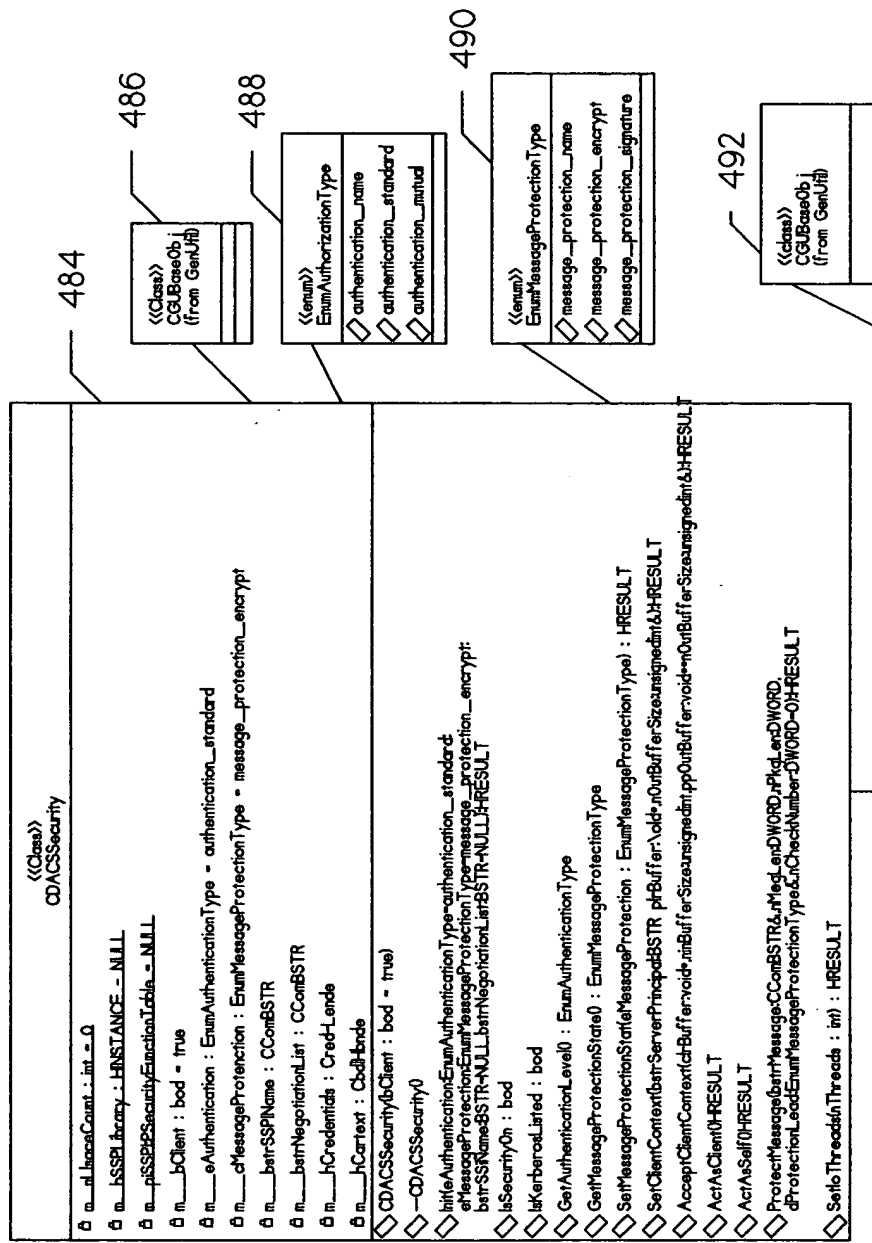
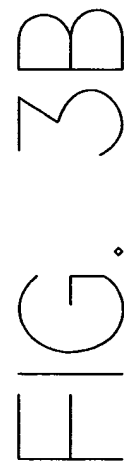


FIG. 2





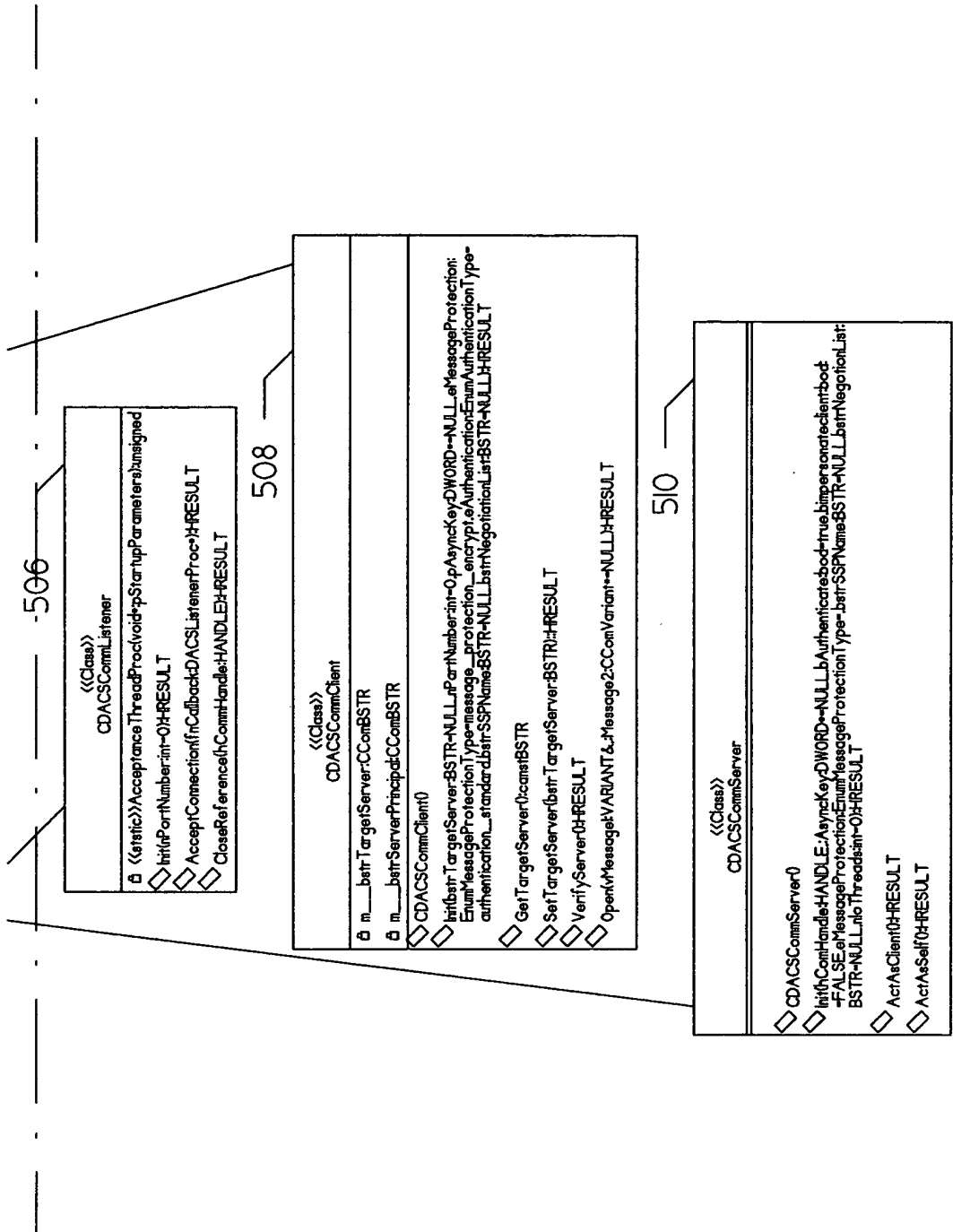


FIG. 3C

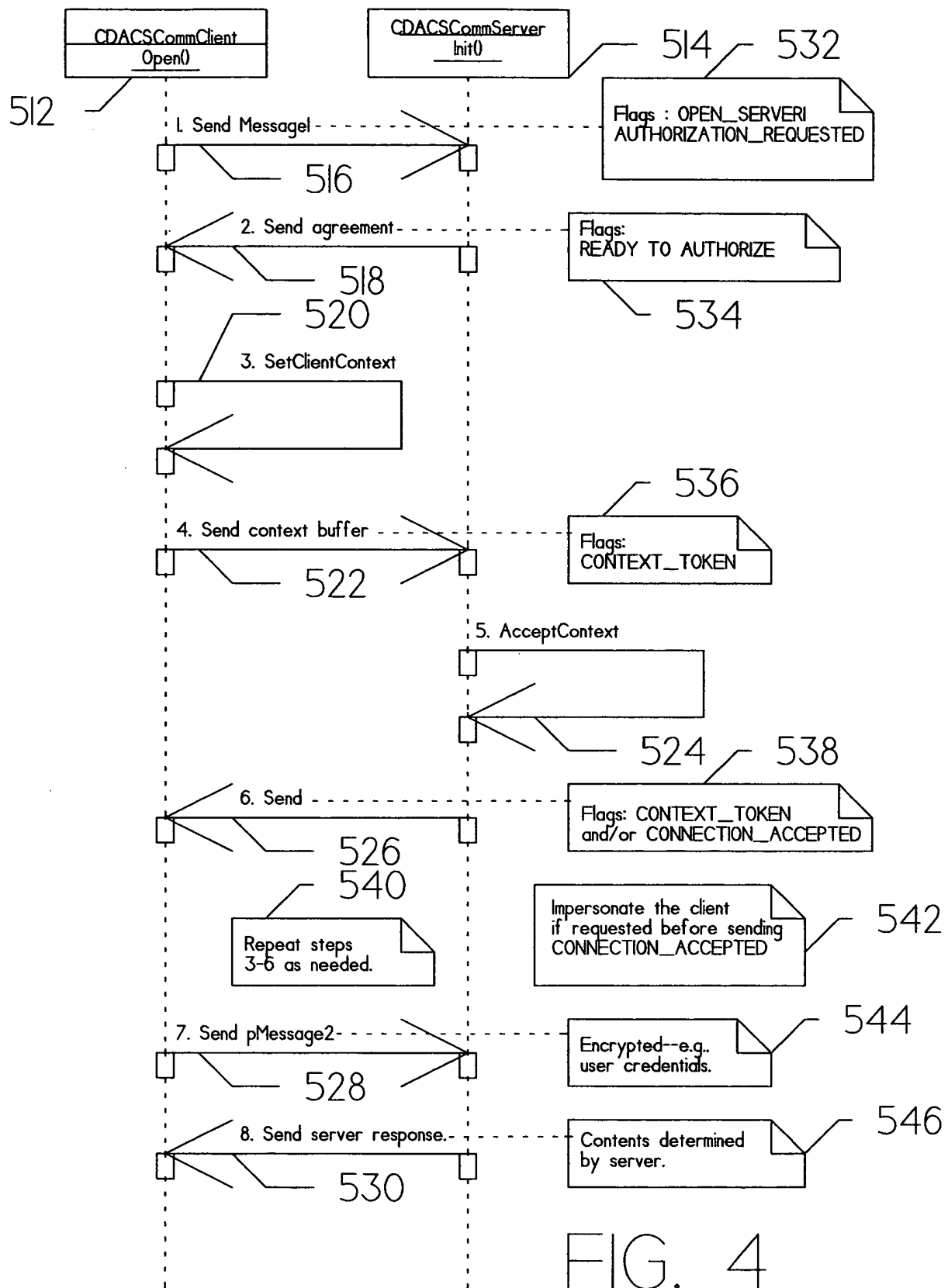


FIG. 4

Message #	Description	Fig. 16 Reference
1	After the connection has been accepted, send the caller's initial message. This message is not encrypted.	516
2	If authorization is requested and agreed by the server, tell client that the server is ready for its security context. Otherwise, go to step 6.	518
3	Call the SSPI InitializeSecurityContext function to get a context token.	520
4	Send the client context token to the server.	522
5	Call the SSPI AcceptSecurityContext function with the buffer received from the client.	524
6	This step depends on the SSP. Set the CONTEXT_TOKEN flag if AcceptSecurityContext provided an output buffer. If it returned SEC_E_OK, impersonate the client if so requested by the server consumer, and set the CONNECTION_ACCEPTED flag.	526
7	Since vMessage1 is sent unencrypted, the client may provide a second message to send encrypted.	528
8	Open attaches the server response to the pMessage2 parameter as output. The consumer client should check both the return value from Open and the contents of pMessage2 if used.	530

FIG. 5